

RY-LGSP38-28

Switch 19" avec gestion, fonctions de sécurité fortes et PoE+

- Switch L2/L3 19" avec PoE+
- Ports en cuivre : 24 x10/100/1000TX
- Ports fibre optique : 4 x SFP/SFP+ 1G/10G
- Manageable, boucle redondante, routing statique et dynamique
- OSPFv2/v3 und RIPv1/v2
- PoE Non Stop
- Ventilateur réglé
- Alimentation 230VAC



Ce switch de layer 2 et de layer 3 a été spécialement conçu pour les applications à forte charge de données, comme par exemple la vidéo sur IP, le streaming vidéo, également en combinaison avec le multicast. Le switch dispose de fonctions de sécurité étendues qui protègent le switch lui-même ainsi que le trafic réseau. Grâce au PoE, les caméras IP peuvent être alimentées via le câble de données. Les possibilités de gestion étendues permettent de répondre aux exigences les plus complexes en matière de réseau.

Fonction spéciale pour les réseaux vidéo

Surveillance active de la caméra

Les caméras alimentées par le switch via PoE sont surveillées en permanence. En cas de panne d'une caméra, le switch redémarre automatiquement la caméra. En cas d'échec, le switch envoie un message d'alarme via SNMP.

Surveillance active de l'alimentation PoE

En cas qu'une caméra défectueuse exige trop d'énergie de la part du switch, une alerte via SNMP est émise.

Gestion active de la performance du PoE

Lors du démarrage du Switch, les différents ports PoE peuvent être mis en service décalé pour éviter la surcharge du bloc d'alimentation PoE.

Intégration active du switch dans les systèmes de gestion vidéo

Pour les systèmes de gestion vidéo populaires Milestone et Siveillance Video, des modules SW sont disponibles, qui permettent une intégration directe de la gestion du switch et du DMS dans ce VMS.

Alimentation PoE ininterrompue

L'alimentation en PoE des PD n'est pas interrompue lorsque le switch est redémarré.



Des Jumbo Frames également à 100 Mbit/s

Les Jumbo Frames jusqu'à 10'240Bytes sont également supportés à 100MBit/s.

Plus d'information

Propriétés spéciales	<p>Le switch a des fonctions de sécurité étendues. Par exemple, l'ACL permet de protéger non seulement le switch lui-même, mais aussi le trafic dans le réseau.</p> <p>PoE non-stop : lorsque le switch est redémarré, l'alimentation PoE des caméras connectées n'est pas interrompue. Dès que le switch est à nouveau opérationnel, les images des caméras le sont aussi.</p>
----------------------	---

DMS

DMS (Device Management System), Système de gestion des appareils

Le switch est équipé d'un système intégré de surveillance du réseau, ce qui donne à l'utilisateur une bonne vue d'ensemble du réseau de manière très simple. Ce système DMS a les caractéristiques suivantes :

Vue d'ensemble du réseau graphique

La vue topologique du réseau offre une vue d'ensemble rapide de tous les switches et appareils terminaux du réseau, tels que les caméras IP ou les serveurs, en indiquant l'adresse IP, le type et le nom de l'appareil. Les plans et les cartes peuvent être stockés sous forme d'images de fond, ce qui permet à l'utilisateur d'accéder rapidement à certains appareils du réseau, même s'il ne connaît pas l'adresse IP.

Recherche de dispositif

Cette fonction permet d'accéder à un appareil spécifique dans les grands réseaux. Les nouveaux dispositifs récemment ajoutés, tels qu'une caméra IP remplacée, sont affichés instantanément et permettent à l'utilisateur d'accéder immédiatement au dispositif sans connaître l'adresse IP.

Affichage du trafic de données

Le trafic de données peut être affiché graphiquement pour chaque port sur un axe temporel.

Dépannage et sécurité

Diagnostic du réseau entre le master switch et les appareils connectés.

Des mécanismes de protection tels que la limitation du débit de données permettent une protection efficace contre les accès non désirés.

IEEE802.3ah et IEEE802.1ag offrent des outils pour structurer des réseaux.



Données techniques

Propriétés générales

Tension d'alimentation	100-240VAC, 50-60Hz
Puissance absorbée	Max. 40W (sans PoE) / 410W (avec PoE)
MTBF	25°C: 188'146h 50°C: 59'932h
Température de service	0°C à 50°C
Dissipation de puissance	136BTU, valeur sans tenir compte de la puissance PoE. 239 BTU, à la puissance maximale de 370W du PoE
Dimensions	442 x 211 x 44mm (LaxLoxHa)
Poids	2.8 kg

Interfaces

Ports en cuivre	24 x 10/100/1000TX, PoE+, RJ45 Puissance PoE maximale pour tous les ports: 370W
Ports fibre optique	2 x SFP/SFP+, 1G/10G Nous recommandons l'utilisation de nos SFPs barox. La compatibilité de nos appareils avec les SFP d'autres marques n'est pas testée et n'est pas garantie par nous.
Port console	1 x RS232, RJ45



Propriétés de réseau

Management	HTTP/HTTPS, SSH, Telnet Client, IPv6 Management SNMP v1, v2c, v3 soutient les trappes et l'USM DHCP Client / DHCPv6 Client DHCP Server Embedded RMON-Agent soutient les groupes RMON 1,2,3,9 (histoire, statistiques, alarmes et événements) pour une meilleure gestion, surveillance et analyse du trafic
Backplane	128Gbit/s
Mac-table	32k
Configuration	Web GUI, DMS, SNMPv1, v2c und v3, console, Telnet, RMON Les accès individuels à la gestion peuvent être désactivés
PoE Management	Configuration du port Supporte la fonction de configuration PoE par port. Scheduling du PoE Soutient la programmation PoE par port pour mettre en marche/arrêter les dispositifs PoE (PD) Contrôle automatique Vérifiez l'état de connexion des PD. Relancez les PD s'il n'y a pas de réponse. Retard de puissance Les ports PoE peuvent être activés avec une temporisation pour protéger le switch contre les surcharges. PoE non stop, redémarrage soft Le switch alimente les PD en énergie même pendant le redémarrage soft.
Configurations de ports	Port disable/enable, Autonegotiation 10/100/1000Mbps, Flow Control disable/enable, contrôle du débit de données sur chaque port, max. Framesize, Power Control
État port	Affichage par port : Débit de données, Link Status, Flow Control Status, Autonegotiation Status, Trunk Status
Fonctions layer3	IPv4 et IPv6 Unicast : routage statique RIP v1/v2 : le protocole d'information de routage (RIP) est un protocole de routage interne basé sur le routage par vecteur de distance et utilisé au sein d'un système autonome. OSPF v2/v3 : OSPF est un protocole de routage à l'état de lien. Il est conçu pour un fonctionnement interne dans un système autonome unique. Chaque routeur OSPF maintient une base de données identique qui décrit la topologie du système autonome. Une table de routage est calculée à partir de cette base de données en créant un arbre de chemins les plus courts.



Redondance de communication

Standard Spanning Tree (STP), IEEE802.1d
Rapid Spanning Tree (RSTP), IEEE802.w
Multiple Spanning Tree (MSTP), IEEE802.1s

Vlan

VLAN à base de tags selon 802.1Q
Supporte jusqu'à 4K VLANs simultanément

VLAN basé au port

Un port membre d'un VLAN peut être isolé des autres ports isolés du même VLAN et des VLAN privés.

VLAN-Edge privé (PVE)

Les VLAN privés sont basés sur le masque de port source et il n'y a pas de connexion aux VLAN. Cela signifie que les ID VLAN et les ID VLAN privés peuvent être identiques.

Voix VLAN

La fonction VLAN vocal vous permet de router le trafic vocal sur le VLAN vocal.

VLAN guest

Avec la fonction VLAN guest IEEE 802.1X, un VLAN guest peut être configuré pour chaque port 802.1X de l'appareil afin de fournir des services limités aux clients non conformes à la norme 802.1X.

Q-in-Q (double tag) VLAN

Cela vous permet de définir des exigences spécifiques pour les ID VLAN et le nombre de VLAN à prendre en charge.

Protocole 802.1v VLAN

La classification de plusieurs protocoles dans un seul VLAN fait souvent respecter des limites de VLAN qui ne conviennent pas à certains des protocoles. Cela nécessite la présence d'une unité non standard qui transmet les cadres contenant les protocoles pour lesquels les limites des VLAN ne sont pas adaptées entre les VLAN.

VLAN basé sur MAC

La fonction VLAN basée sur MAC permet d'attribuer des paquets entrants non marqués à un VLAN, en classant le trafic en fonction de l'adresse MAC source du paquet.

VLAN basé sur le sous-réseau IP

Dans un VLAN basé sur un sous-réseau IP, tous les postes de travail finaux d'un sous-réseau IP sont affectés au même VLAN. Dans ce VLAN, les utilisateurs peuvent déplacer leurs postes de travail sans avoir à reconfigurer leurs adresses réseau.

VLAN gestion

Le VLAN de gestion est utilisé pour gérer le commutateur à partir d'un emplacement distant en utilisant des protocoles tels que Telnet, SSH, SNMP, Syslog, etc.

Agrégation de connexion

IEEE 802.3ad LACP / Static Trunk, supporte cinq groupes de troncs à 16 ports ou troncs statiques.



Qos

File d'attente hardware
Supporte huit files d'attente hardware.

Classification

Basé sur le port : QoS du trafic par port

802.1p : La classe de service CoS QoS de couche 2 basée sur la priorité du VLAN est un paramètre utilisé dans les protocoles de données et de voix pour distinguer les types de charges utiles contenues dans le paquet transmis.

QoS DSCP de la couche 3 des services différenciés basés sur le DSCP (DiffServ) : les paquets IP peuvent porter soit une valeur de priorité IP (IPP), soit une valeur DSCP (Differentiated Services Code Point). La QoS permet l'utilisation des deux valeurs car les valeurs DSCP sont rétrocompatibles avec les valeurs de priorité IP.

Classification et ré-étiquetage des LCA TCP/IP : QoS par le biais de l'ACL

Limitation des taux

Ingress Policer

Egress-Shaping et contrôle de taux des données par port

Scheduling

Priorité stricte et round robin pondéré (WRR) : Le round robin pondéré est un algorithme de planification qui utilise les poids attribués aux files d'attente pour déterminer la quantité de données qui est éliminée d'une file d'attente avant d'être déplacée vers la file suivante.



Sécurité

Authentification certifiée

Il est possible d'enregistrer une clé HTTPS privée pour l'accès à la gestion.

Gestion des utilisateurs

Les droits des utilisateurs peuvent être définis librement sur 15 niveaux au maximum.

ACL

Le switch permet jusqu'à 512 entrées. Limitation du drop ou du débit basée sur l'adresse MAC/IP source/cible ou l'ID VLAN. Des règles et des conditions peuvent être définies par port pour les paquets entrants. Les règles comprennent les protocoles, les ports IP et les plages d'adresses. Les règles peuvent être définies au choix selon la méthode d'autorisation ou d'exclusion. Les critères sont les suivants : Ports source et destination TCP/ UDP, priorité 802.1p, type Ethernet, paquet ICMP (Internet Control Message Protocol).

Sécurité des ports

Gestion des adresses MAC par port et IP-Source-Guard : l'adresse MAC peut être contrôlée en combinaison avec l'adresse IP.

Storm Control

Empêche que le trafic d'un LAN soit perturbé par un flot de diffusion, de multidiffusion ou de monodiffusion sur un port.

Authentification RADIUS, 802.1X

Autorisation et facturation, hachage MD5, VLAN invité, mode hôte unique/multiple et sessions uniques/multiples.

Supporte 802.1X basé sur IGMP-RADIUS

Attribution dynamique de VLAN

Authentification TACACS

Le switch prend en charge l'authentification TACACS+. Le commutateur en tant que client.

Secure Shell (SSH)

SSH sécurise le trafic Telnet entrant ou sortant du commutateur, SSH v1 et v2 sont pris en charge.

Secure Socket Layer (SSL)

SSL crypte le trafic HTTP et permet ainsi un accès sécurisé étendu à l'interface utilisateur graphique de gestion basée sur un navigateur dans le commutateur.

HTTPS & SSL (Web sécurisé)

Hyper Text Transfer Protocol Secure (HTTPS) est la version sécurisée de HTTP.

BPDU Guard

Le BPDU Guard, une extension de STP, supprime un nœud qui reflète les BPDUs vers le réseau. Il fait respecter les limites du domaine STP et maintient la prévisibilité de la topologie active en ne permettant pas aux appareils réseau situés derrière un port compatible avec BPDU Guard de participer à STP.

Snooping DHCP



Avec DHCP Snooping, le switch possède une fonction qui fait office de pare-feu entre les hôtes non fiables et les serveurs DHCP fiables.

Protection de boucle

La protection des boucles permet d'éviter les boucles de monodiffusion, de diffusion et de multidiffusion inconnues dans les configurations de commutation de couche 2.

Multicast

IGMP v1/v2/v3 Snooping

L'IGMP limite le trafic multicast à forte intensité de bande passante aux candidats. Prend en charge 1024 groupes multicast.

IGMP Querier

IGMP Querier est utilisé pour prendre en charge un domaine multicast de couche 2 de switchs snooping lorsqu'aucun routeur multicast n'est disponible.

Proxy IGMP

IGMP Snooping avec rapport de proxy ou suppression de rapport filtre activement les paquets IGMP pour réduire la charge sur le routeur multicast.

MLD v1/v2 Snooping

Délivre des paquets multicast IPv6 uniquement aux destinataires requis.

Enregistrement de VLAN multidiffusion (MVR)

Un VLAN dédié, configuré manuellement, appelé VLAN Multicast, pour acheminer le trafic multicast sur un réseau de couche 2 en conjonction avec le snooping IGMP.

Normes

IEEE 802.3 10Base-T
IEEE 802.3u 100Base-TX/100BASE-FX
IEEE 802.3z Gigabit SX/LX
IEEE 802.3ab Gigabit 1000T
IEEE 802.3x Flow Control and Back pressure
IEEE 802.3ad Port trunk with LACP
IEEE 802.1d Spanning tree protocol
IEEE 802.1w Rapid spanning tree protocol
IEEE 802.1s Multiple spanning tree protocol
IEEE 802.1p Class of service
IEEE 802.1Q VLAN Tagging
IEEE 802.1x Port Authentication Network Control
IEEE 802.1ab LLDP
IEEE 802.3af/at Power over Ethernet
IEEE 802.az Energy Efficient Ethernet

Variantes du produit



RY-LGSP38-28

Version 28.08.2023, Sous réserve de modifications